AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

Plaintiff,

v.

REBECCA SILVEYRA,

Defendant.

Case No. 8:22-mj-00334-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of August 7, 2021 in the county of Orange in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1344(2)	Bank Fraud

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Loren Rofe
Complainant's signature

Loren Rofe, United States Postal Inspector
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: May 3, 2022

Karen E. Scott
Judge's signature

City and state: Santa Ana, California

Hon. Karen E. Scott, U.S. Magistrate Judge
Printed name and title

AUSA: Benjamin Barron (714-338-3536)

AFFIDAVIT

I, Loren Rofe, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Postal Inspector with the United States Postal Inspection Service ("USPIS") and have been so employed since March 2001. I currently am assigned to the Los Angeles Division, Mail Theft Team located in Long Beach, California. The Mail Theft Team investigates postal-related crimes, including theft of United States mail ("U.S. mail"), fraud, and related activity in connection with access devices that include credit cards and debit cards, identity theft, and unauthorized use of other persons' information for financial gain. The Mail Theft Team also investigates crimes related to the use, theft, or counterfeiting of postal keys (referred to as "arrow keys") and locks. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7). As such, I am empowered to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

2. I have completed a sixteen-week, basic training course in Potomac, Maryland, which included training in the investigation of mail theft, identity theft, and crimes against postal property. During my employment, I have investigated crimes involving mail theft, bank fraud, identity theft, credit card fraud, and the theft or counterfeiting of postal keys and

locks. I have interviewed suspects, victims, and witnesses regarding mail theft, bank fraud, identity theft, and the theft or counterfeiting of postal keys. Based on my own mail theft investigations and discussions with other Postal Inspectors, who combined have over 20 years of experience, I have learned about mail theft investigations and common mail theft and identity theft practices. Prior to being assigned to the Mail Theft Team, I was assigned to the Prohibited Mailing Narcotics Team in Los Angeles, California where my duties included investigating narcotics violations involving the United States Mails. From January 1996 to March 2001, I was previously employed as a Special Agent with the United States Immigration and Naturalization Service, which later became part of the US Department of Homeland Security. In this capacity I enforced Immigration laws throughout Southern California. I was also assigned to investigate violent street gangs. In that assignment, I worked both independently and in a task force where I led and participated in investigations related to crimes perpetrated by members of violent street gangs.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a criminal complaint and arrest warrant for REBECCA SILVEYRA ("SILVEYRA") for a violation of 18 U.S.C. § 1344(2) (Bank Fraud) on or about August 7, 2021, as described further below.

4. This affidavit also is made in support of an application for warrant to search the residence located at 2901

Nutwood Avenue, Apartment C14, Fullerton, CA 92831 ("SUBJECT PREMISES"), as described more fully in Attachment A, which is incorporated by reference herein.

5. The requested search warrant seeks authorization to seize the evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1708 (Possession of Stolen Mail), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1029(a)(2) (Use of Unauthorized Access Device), and 18 U.S.C. § 1028(A) (Aggravated Identity Theft) (collectively, the "SUBJECT OFFENSES"), as more fully described in Attachment B, which is incorporated by reference herein.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrant, and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUMMARY OF PROBABLE CAUSE

7. Starting on or about June 2021, SILVEYRA used the stolen California Driver's license of victim "A.F." to fraudulently obtain credit and make purchases. In August 2021, incoming and outgoing checks belonging to Underhill

International were stolen out of the United States Mail and fraudulently deposited into Bank of America and Citibank accounts, both of which are FDIC insured financial institutions. As further described below, my investigation has revealed that SILVEYRA was the individual who opened personal and business accounts at Bank of America and Citibank. Regarding the Citibank account, SILVEYRA opened the personal account under the name of A.F. but opened the business account under the name Underhill International. SILVEYRA then deposited the incoming checks stolen from the true Underhill International into her Citibank account. SILVEYRA also opened personal and business accounts with Bank of America. The personal account was opened under the name A.F. and the business account was opened under the name Zephyr Networks. Both accounts were utilized for depositing outgoing checks belonging to Underhill International. The approximated loss to Underhill International is $192,000.00. The single count charged in the requested complaint focuses on SILVEYRA's August 7, 2021 deposit of a $108,448.80 check issued by victim Underhill International into a Bank of America account held in the name of identity theft victim A.F., as described further below.

IV. STATEMENT OF PROBABLE CAUSE

A. Fraudulent Bank Deposits and Identity Theft

8. Based upon my conversations and correspondence with United States Postal Inspectors, United States Postal Service Office of Inspector General Special Agents, conversations with

victims, reviewing of Bank of American and Citibank records, and reviewing reports from the Costa Mesa and Fullerton Police Departments, I am aware of the following facts:

a. On August 4, 2021, an individual later identified as SILVEYRA opened a Bank of America account ending in 2422 under the business name Zephyr Networks. On August 6, 2021, SILVEYRA opened Bank of America accounts ending in 5047 and 2011 in the name of identity theft victim A.F. To open the accounts, SILVEYRA provided Bank of America stolen California Driver's license number XXXX9380 belonging to A.F. The address provided to Bank of America to open the account was 2901 Nutwood Ave., Apt. C14, Fullerton, CA, that is, the SUBJECT PREMISES, which as further described herein is SILVEYRA's residence.

b. Between June 2021 and August 2021, Underhill International located at 15251 Barranca Parkway, Irvine, CA experienced a recurring problem of mail theft from their secured mailbox unit. Both incoming and outgoing mail including numerous checks were stolen from the company's mailbox. On August 5, 2021, the company placed several vendor payment checks in their mailbox unit to be mailed out. On August 12, 2021, E.U., the owner of Underhill International, was contacted by Bank of America regarding two checks that had been issued by the company, both of which had been deposited into an account described above later determined to have been opened by SILVEYRA. Bank of America provided E.U. copies of both checks. The first check #30223 was issued on August 5, 2021, in the

amount of $108,448.80 made payable to ContiTech USA. The check posted on August 9, 2021. The second check #30230 was also issued on August 5, 2021, in the amount of $4,487.07 made payable to Storm Manufacturing Group, Inc. The check posted on August 12, 2021. Both checks were endorsed with the name A.F. On February 10, 2022, I obtained account records and surveillance photos from Bank of America which showed the following:

i. On August 7, 2021, Underhill International check #30223 in the amount of $108,448.80 was deposited through the teller at the Brea branch located at 290 S. State College, Brea, CA. Check number 30223 was deposited into the account ending in numbers 2011 belonging to A.F ("hereinafter referred to as the A.F. account").

ii. On August 12, 2021, Underhill International check #30230 in the amount of $4,487.07 was mobile deposited into account ending in numbers 2422 belonging to Zephyr Networks ("hereinafter referred to as the Zephyr Networks' account").

iii. On August 11, 2021, a teller transfer of $70,000 from the A.F. account to Zephyr Networks' account was conducted at the Brea Branch.

iv. On August 11, 2021, three withdrawals were conducted from the Zephyr Networks' account at three different Bank of America branches totaling $70,000.00. More specifically, a $50,000.00 teller withdrawal was conducted at the Placentia branch located at 160 E. Yorba Linda Blvd., Placentia, CA. A $10,000.00 teller withdrawal was conducted at

the Yorba Linda branch located 4802 Main Street, Yorba Linda, CA, and a $10,000.00 teller withdrawal was conducted at the Anaheim Hills branch located at 5640 E. Santa Ana Canyon, Anaheim, CA.

v. On August 11, 2021, a $30,030.00 teller withdrawal was conducted from the A.F. account at the Bank of America Brea branch located at 290 S. State College, Brea, CA. The withdrawals consisted of the purchasing of two cashier's checks each totaling $10,000.00 with a $30.00 check fee, and a $10,000.00 cash withdrawal.

vi. On August 11, 2021, an $8,000.00 teller withdrawal was conducted at the Yorba Linda branch from the A.F. account and then transferred to the Zephyr Networks' account.

vii. Bank of America provided surveillance photos for the August 7, 2021, $108,448.80 deposit at the Brea branch, the August 11, 2021, $70,000.00 transfer at the Brea branch, the August 11, 2021, $50,000.00 teller withdrawal at the Placentia branch, the August 11, 2021, $10,000.00 teller withdrawal at the Anaheim Hills branch, the $30,030.00 teller withdrawal at the Brea branch, and the $8,000.00 withdrawal/transfer at the Yorba Linda branch. As discussed further below, I have compared the surveillance photos provided by Bank of America with SILVEYRA's California Department of Motor Vehicles ("CA DMV") photograph, and recognize that SILVEYRA is the person shown conducting the bank transactions.

c. In August 2021, Underhill International's incoming mail, which included numerous checks from clients, was also stolen from the company's mailbox unit. Underhill International contacted clients when they did not receive payment. The clients informed Underhill International that the checks had successfully shown paid to Underhill International.

d. On September 1, 2021, Underhill International was contacted by Citibank and informed that an account was opened in Underhill International's name and approximately twenty checks were deposited into that account. Funds from the account were subsequently withdrawn.

e. On March 21, 2022, I obtained account records from Citibank which informed me of the following:

i. On August 17, 2021, an individual listing a name of A.F. and a Doing Business AS ("DBA") Underhill International completed a Business Deposit Account Application and opened account ending in numbers 2325.

ii. The individual provided a copy of California Driver's License #XXXX9380 in the name of A.F., Social Security Number XXX-XX-1666 belonging to A.F., and listed an address of 2901 Nutwood Avenue, Apartment C14, Fullerton, CA 92831 (the SUBJECT PREMISES).

iii. Between August 20, 2021, and August 30, 2021, twenty checks totaling approximately $79,889.00 made payable to Underhill International were deposited into Citibank

account 2325. Between August 2021 and September 1, 2021, no less than $50,000.00 was withdrawn from the account.

f. On March 7, 2022, I received Costa Mesa Police Department ("CMPD") Report Number 21-016989. The report provided the following information:

i. On October 14, 2021, CMPD Officer M. Evans met with victim A.F. to take an identity theft report.

ii. A.F. informed Officer Evans that her California Driver's license was stolen from her mailbox when she lived at her previous residence in Huntington beach.

iii. In June 2021, A.F. noticed a change in her email and information with her unemployment benefit's account. A.F. conducted a credit check through Experian and learned that on August 14, 2021, a vehicle was purchased through Toyota Motor Credit in A.F.'s name. A.F. then checked her Wells Fargo bank account online and observed withdrawals and deposits she did not make, including a $12,621.91 deposit.

iv. On October 27, 2021, CMPD Investigator J. Dance spoke with Toyota/Lexus Financial Services Fraud Investigator G. Munson. Investigator Munson confirmed for Investigator Dance that a vehicle was purchased on August 14, 2021, at the South County Lexus in Mission Viejo, CA.

v. On October 28, 2021, Toyota/Lexus Fraud Investigator A. Smith provided Investigator Dance with the "dealer jacket" for the vehicle purchase which included the following documents:

(I) Progressive Insurance card and verification for insurance for policy number 950514016 in the name of A.F.

(II) Copy of the front and back of California Driver's license number XXXX9380 in the name of A.F.

vi. On October 28, 2021, Investigator Dance used a law enforcement database and searched A.F.'s name for registered vehicles and located the fraudulently purchased vehicle, a 2014 Lexus, with license plate CA #8XRM349, Vehicle Identification Number ("VIN") #JTHFF2C2E2530541.

vii. While reviewing the "dealer jacket", Investigator Dance observed three vehicle identification numbers VINs listed on the Progressive insurance card: a 2009 Infiniti – JNKCV66E19M723154; a 2013 Buick – 1G4PS5SK5D4109178; and a 2013 BMW – WBA3C1C58DF440761. Investigator Dance again used law enforcement databases and searched VIN #JNKCV66E19M723154. The VIN returned to a 2009 Infiniti registered to SILVEYRA at 2901 Nutwood Avenue, Apt. C14, Fullerton, CA (the SUBJECT PREMISES). Investigator Dance also reviewed the copy of California Driver's license number XXXX9380 in the name of A.F. that was in the dealer jacket and compared it to A.F.'s authentic California Driver's license photo. The photo of the license located in the dealer jacket did not appear to be A.F. Investigator Dance then compared the photo in the dealer jacket to SILVEYRA's California Driver's license #XXXX1192, and the photographs appeared to be the same person.

g. On March 7, 2022, I obtained CMPD report #21-017161. The report provided the following information:

i. On October 16, 2021, CMPD Officer Foxwell responded to Nordstrom's Department store. Nordstrom's Department Store Loss Prevention stopped Chelsea Sapp and SILVEYRA after they exited the store for shoplifting. After stopping the two women, Loss Prevention Manager J. Segura searched the Nordstrom's bag that SILVEYRA carried out of the store. The bag contained nine items with the tags still on them that had not been paid for. The magnetic security sensors had been removed from the items. The total retail price of the items stolen was $1,729.35. When Officer Foxwell questioned SILVEYRA she provided California Driver's license #XXXX9380 in the name of A.F. SILVEYRA also verbally told Officer Foxwell her name was A.F. SILVEYRA was in possession of Fidelity Cash Management Account Visa Debit card #XXXX XXXX XXXX 8611, Current Visa Debit card #XXXX XXXX XXXX 9117, and Social Security card #XXX-XX-1666, all bearing the name A.F.

ii. Both Chelsea Sapp and SILVEYRA were arrested by Officer Foxwell for burglary, in violation of 459 PC; grand theft, in violation of 487(a) PC; and conspiracy, in violation of 182(a)(1) PC.

iii. Officer Foxwell received a phone call from the Costa Mesa Jail staff who informed him that SILVEYRA's prints did not match the name she provided, A.F. and that

SILVEYRA had now provided her true name. SILVEYRA's identity was also confirmed through Cal-DOJ by her fingerprints.

iv. Investigator Dance reviewed Officer Foxwell's report and recognized SILVEYRA as the same individual responsible for purchasing the 2014 Lexus using A.F.'s identification.

h. On March 7, 2022, I compared SILVEYRA's California Driver's license photo XXXX1192 to the surveillance photos provided by Bank of America. SILVEYRA appears to be the person in all the Bank of America photos conducting the transactions. The residential address listed for SILVEYRA on her driver's license is 2901 Nutwood Ave., Apt. C14, Fullerton, CA (the SUBJECT PREMISES). This is the same address SILVEYRA provided when she opened the Bank of America and Citibank accounts. It is also the same address SILVEYRA originally wrote down, before crossing it out and replacing it with the former address of A.F., on the credit application she completed to purchase the Lexus.

B. Victim Interviews

9. On September 27, 2021, I interviewed victim E.U., who informed me of the following:

a. E.U. is the owner of Underhill International. On August 5, 2021, the company mailed out numerous checks as payments to vendors. On August 12, 2021, E.U. received a call from Bank of America regarding a check belonging to Underhill International made payable to ContiTech USA, in the amount of

approximately $108,000.00. E.U. further stated he was informed by Bank of America that the endorsee for the check was someone by the name of A.F. and the check was deposited into A.F.'s account. E.U. also believed another check was stolen by the same individual because Bank of America informed him that it was also endorsed by A.F. Bank of America informed E.U. that money had been withdrawn from the accounts, but E.U. could not remember the total amount.

b. E.U. also contacted all the vendors that Underhill International had mailed checks to and learned that none had received their payments. E.U. also contacted Underhill International customers due to not receiving payments owed to the company. All the customers confirmed they had mailed out their payments and they had cleared with Underhill International as the payee.

c. On September 1, 2021, E.U. spoke with Citibank and learned that approximately twenty checks had been deposited into an account opened under the name A.F. with a DBA of Underhill International. E.U. confirmed that Underhill International banks with Bank of American and does not possess an account with Citibank. E.U. believed the checks deposited into the fraudulently opened Citibank account were inbound checks stolen from the company's mailbox. E.U. believed A.F. opened a Citibank account under the name Underhill International for the sole purpose of stealing the company's checks and depositing them into a fraudulently obtained account that

appeared legitimate. Citibank also informed E.U. that approximately $60,000.00 in checks made payable to Underhill International had been deposited and withdrawn from the account.

d. E.U. confirmed he does not know A.F. and A.F. was never authorized to possess, retain, or use anything associated to the company, including, but not limited to its checks. Underhill International also does not do business with A.F. or Zephyr Networks. A.F. was also never authorized to open any account in the Underhill International name.

10. On March 4, 2022, I interviewed victim A.F., who informed me of the following:

a. In September or October 2020, A.F. never received her new California Driver's license. A.F. did not think anything of it until around June 2021, when she noticed suspicious activity with her Wells Fargo account, and changes in her email and with her unemployment benefit's account. A.F. believes that in June 2021, someone posing as A.F. was able to get access to her Wells Fargo account and obtain a debit card and the PIN to her account. A.F. then noticed that a Wells Fargo business account she never applied for was attached to her personal account, but she did not have access to it. A.F. could only view the account online and noticed a deposit of approximately $12,000.00 in the business account. At the same time, A.F. noticed $700.00 withdrawn from her Wells Fargo checking account and $300.00 from her savings account. A.F. filed a report with Wells Fargo and had the account frozen.

b. A.F. conducted a credit check with Experian and learned a Lexus was purchased on August 14, 2021, through Toyota Motor Credit in her name. A.F. stated the loss through Toyota Motor Credit was approximately $26,000.00.

c. On August 17, 2021, A.F. was contacted by D. Song, the owner of Forte Strings, a music instrument store, where a person posing as A.F. purchased a $7,000.00 violin. Ms. Song told A.F. that SILVEYRA asked her if she could make payments on the violin and provided a Bank of the West check in A.F.'s name in the amount of $2,542.50. The address listed on the check was 2901 Nutwood Ave., Apt. C14, Fullerton, CA (the SUBJECT PREMISES). She also provided a Bank of America Visa debit card #XXXX XXXX XXXX 8095 in the name of A.F. and Zephyr Networks. Ms. Song also informed A.F. that when she could not process the check payment, she contacted Bank of the West and was informed the check was fictitious. A.F. confirmed that she has never opened or possessed Bank of the West or Bank of America accounts. A.F. also confirmed she has never lived at 2901 Nutwood Avenue, Apt. C14, Fullerton, CA. When Ms. Song learned the purchase was fraudulent, she contacted the true A.F. through social media and informed her about the violin purchase. A.F. confirmed for Ms. Song that she was not the person who purchased the violin. Ms. Song then sent A.F. photos of SILVEYRA in the store making the purchase, a photo of the check used to make a partial payment, a photo of a Bank of America Business Visa debit card in A.F.'s name, and a photo of

SILVEYRA's license plate CA #BS44F38 as she drove away. I have reviewed the surveillance photograph and license plate and recognize that they show SILVEYRA. A.F. stated the vehicle SILVEYRA drove was the Lexus she purchased in A.F.'s name.

d. A.F. was then shown photos of SILVEYRA conducting the Bank of America transactions. A.F. stated she did not know the person and she did not have permission to possess, retain, or use any of A.F.'s personal identifying information, or apply for any type of credit in A.F.'s name.

11. On March 7, 2022, using law enforcement databases, I conducted a check of temporary license plate CA #BS44F38 which was the license plate number Ms. Song took a photo of as SILVEYRA drove away from her business. The permanent license plate number assigned to the vehicle is CA #8XRM349. I then queried license plate CA #8XRM349. The vehicle is a 2014 Lexus (VIN: JTHFF2C23E2530541) and is registered to A.F. at 8102 Ellis Avenue, #305, Huntington Beach, CA 92646. This is the same vehicle that SILVEYRA fraudulently purchased in A.F.'s name, as described above.

B. Additional Investigation

12. On March 15, 2022, I went to the Moonraker Apartments located at 2901 Nutwood Ave, Fullerton, CA and spoke with the property manager. The Property manager informed me of the following:

a. SILVEYRA has lived in apartment C14 (the SUBJECT PREMISES) continuously since September 4, 2020. A.F. has not lived at the apartment complex.

b. On November 30, 2021, a gas inspection was conducted at apartment C14 in which the property manager was present with the gas inspector. During the inspection, the gas inspector found a hidden camera by the heating unit, and the property manager observed four high-end possibly commercial grade printers all operational within one area of the apartment. Based on my training and experience, I have learned that mail/identity thieves will use commercial grade computers and printers to create checks and print counterfeit credit and identification cards, such as the California Driver's license SILVEYRA provided to South County Lexus that contained her photo with victim A.F.'s personal information.

c. The property manager also stated that a lot of strange activity continuously occurs within the apartment. The property manager has observed multiple people arriving and leaving with large numbers of boxes and envelopes throughout the day. The activity is ongoing and occurs several days a week, which the property manager thought was odd since, to her knowledge, SILVEYRA is unemployed.

d. SILVEYRA has two vehicles registered with the apartment complex for parking purposes. One of the vehicles is a 2017 Honda CR-V with CA#7YXC801 and the other is a 2009 Infiniti with CA#7URC946.

13. On March 17, 2022, using law enforcement databases I queried license plate CA #7URC946. The vehicle has VIN #JNKCV66E19m723154 and is registered to SILVEYRA at 2901 Nutwood Avenue, Apt. C14, Fullerton, CA (the SUBJECT PREMISES). This is the same vehicle CMPD Investigator Dance found on an insurance card that was provided by SILVEYRA to South County Lexus when fraudulently purchasing the 2014 Lexus using A.F.'s identity, as well as the same address SILVEYRA listed on the Bank of America and Citibank applications.

14. On March 25, 2022, I reviewed Orange Police Department ("OPD") report #22-01-0790 which informed me of the following:

a. On January 25, 2022, Officer M. Roth conducted a vehicle stop of a 2014 Lexus IS 250, license place CA #8XRM349 for a window tint violation. This is the same vehicle SILVEYRA fraudulently purchased in A.F.'s name. Officer Roth contacted the driver, who was later identified as SILVEYRA by her CA DMV photograph. The male passenger inside the vehicle was also identified by his CA DMV photo as Arcadio Lopez.

b. OPD dispatch conducted a records check on SILVEYRA and informed Officer Roth that SILVEYRA was driving with a suspended license.

c As Officer Roth spoke with SILVEYRA, Sergeant McCafferty arrived on scene and assisted. While speaking with SILVEYRA outside of the vehicle, she informed Officer Roth that she had "dope" inside the vehicle but could not remember where. Officer Roth also determined the vehicle would be towed due to

SILVEYRA's license being suspended and then conducted an inventory search of the vehicle prior to tow. While conducting his inventory search, Officer Roth and Sergeant McCafferty located the following items:

i. A backpack located on the backseat of the vehicle behind the driver's seat. Inside the backpack was a California Driver's license ("CDL") belonging to Arcadio Lopez. There was also a Burberry wallet which contained a CDL belonging to "J.M.", multiple credit cards in other people's names, and $2,655.00 in U.S. currency. Also inside the backpack was a pouch which contained multiple containers and small baggies containing a white crystal-like rock resembling methamphetamine, as well as an off-white/brown powdery substance resembling heroin. Near the pouch containing the narcotics, Officer Roth recovered a glass pipe with a bulbous end. He also recovered from the backpack multiple cell phones, and an expandable baton.

ii. In the backseat of the vehicle a large amount of mail that did not belong to SILVEYRA or Arcadio Lopez.

iii. A large duffle bag on the back seat behind the front passenger seat containing clothes and a small pouch which contained a CDL belonging to a person named "R.H.N" and an ID card belonging to a person named "M.B."

iv. A black purse which SILVEYRA stated belonged to her which contained multiple checks for large amounts of money which did not belong to SILVEYRA, and a Wells Fargo bank Visa card in the name of "Y.Q".

d. Officer Roth advised SILVEYRA of her Miranda rights which she stated she understood and agreed to speak with Officer Roth. SILVEYRA informed Officer Roth that the backpack inside the vehicle belonged to a friend named "Al". SILVEYRA stated "Al" uses her car to go "mailboxing". SILVEYRA also stated the purse located in the vehicle and everything inside of it belonged to her, and she did not believe anyone else put any items inside her purse. SILVERYRA was asked about the Wells Fargo bank card belonging to Y.Q. and if she knew SILVEYRA was in possession of her card. SILVEYRA stated Y.Q. would not know the card was in SILVEYRA's possession. When asked about the multiple checks in various names not belonging to her found inside her purse, SILVEYRA admitted they did not belong to her, and she had no idea where they came from. SILVEYRA then changed her original statement and said the purse was not hers and she lied when she said it was her purse.

V. TRAINING AND EXPERIENCE REGARDING THE SUJBECT OFFENSES

15. Based on my training and experience, and consultation with other United States Postal Inspectors, I am aware that typical mail thieves and organized mail theft rings operate as follows:

a. Mail thieves and/or members of the mail theft ring steal mail in a variety of ways: breaking into panel mailboxes at apartment or condominium complexes, which allows the thieves access to numerous individual mailboxes at once; using stolen or counterfeit USPS arrow keys to open USPS

collection or mailboxes; submitting fraudulent U.S. Postal Service "Change of Address" requests to divert mail from a victim's residence and forwarding it to a suspect address or "drop" location; jamming USPS collection boxes with paper, to allow someone to reach into the box; reaching into USPS collection boxes overflowing with U.S. Mail; "mailboxing," a process by which mail thieves drive through neighborhoods and steal outgoing and/or incoming U.S. Mail from residential mailboxes; and "fishing," which is using a homemade sticky device that is lowered into USPS collections boxes to extract U.S. Mail through the deposit slot.

b. Mail thieves and/or members of the mail theft ring will steal U.S. Mail to obtain personal checks, money orders, and cash or other cash equivalents, originally completed and mailed by the true account holders as payment to the account holders' creditors. Mail thieves and ring members often use items or information taken therefrom to commit bank fraud or other financial crimes. Specifically, mail thieves may use the checks to gain financial information including account numbers and account holders' names and addresses. Often, mail thieves use this information to create counterfeit checks, which they make payable to themselves or members of the ring. Mail thieves also may chemically "wash" the checks to remove handwritten information or alter the checks to make them payable to different persons or entities or in higher amounts than originally were written and then fraudulently cashing the

checks. Similarly, mail thieves and/or members of the mail theft ring also steal U.S. Mail to obtain USPS customers' credit cards, credit card statements, credit card convenience checks, and correspondence which contains USPS customers' personal or financial information. The mail thieves use the information from the stolen U.S. Mail to conduct "account takeovers" in which they add their own names to the victims' accounts for the purposes of fraudulently ordering or purchasing merchandise or applying fraudulently for credit cards in the victims' names. Mail thieves also commonly use equipment to print counterfeit credit and identification cards, including equipment to create magnetic strips for credit cards, embossing machines to create credit cards, laser printers to create checks, and magnetic card readers to read and re-encode credit cards.

c. The proceeds generated from the mail theft and related fraud activities often are used to buy methamphetamine or other illegal drugs, which then are used to recruit additional individuals to facilitate the scheme.

d. Mail thieves often keep the evidence, contraband, fruits, or instrumentalities of violations of their crimes in a location that is private, secure, and easily accessible, such as a residence, personal storage units, or inexpensive short-term rental units, such as motel rooms. Mail thieves commonly store in their residence tools that assist in committing their crimes, including but not limited to: stolen U. S. Mail, personal checks and credit cards stolen from the U.S. Mail, notebooks listing

USPS customers' personal information, materials for creating false identification cards, computer equipment, check washing chemicals, equipment to create magnetic strips for credit cards, embossing machines to create credit cards, laser printers to create checks, magnetic card readers to read and re-encode credit cards, tools used to gain access to buildings and/or breaking into panel mailboxes at apartment or condominium complexes, and materials for constructing "fishing" devices. This allows mail thieves to comfortably sort through the stolen mail for valuable items such as checks, money orders, credit cards, credit card applications, and other mail containing personal identifying information.

e. It is also common for mail thieves to keep "profiles" of victims in their residence, including on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, addresses, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers.

f. It is common practice for mail and identity thieves to use and maintain computers to track their fraudulent transactions. These individuals often use computers to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ computers for purposes of, among other things, (1) applying online for fraudulent credit cards;

(2) obtaining personal identification information for the purpose of establishing or modifying fraudulent credit card accounts; (3) using fraudulently obtained credit cards to make purchases; and (4) keeping records of their crimes.

g. Individuals who participate in mail and identity theft use digital devices to maintain telephone numbers of co-conspirators in order conduct their business, to communicate with co-conspirators, and to coordinate their activities.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[1]

16. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the

[1] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain

"booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

17. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

e. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

f. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

18. The search warrant requests authorization to use the biometric unlock features of a device, based on the following,

which I know from my training, experience, and review of publicly available materials:

g. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

h. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

i. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress SILVEYRA's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of SILVEYRA's

face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

19. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII.

17. Based upon the foregoing, I believe that there is probable cause to believe that SILVEYRA has committed violations of 18 U.S.C. § 1708 (Possession of Stolen Mail), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1029(a)(2) (Use of Unauthorized Access Device), and 18 U.S.C. § 1028(A) (Aggravated Identity Theft) (collectively, the "SUBJECT OFFENSES"). Also based on the foregoing, there is probable cause to believe that evidence, contraband, fruits, or instrumentalities of violations of the SUBJECT OFFENSES, as described in Attachment B, will be found in a search of the SUBJECT PREMISES, as described in Attachment A.

/s/ Loren Rofe
Loren Rofé
UNITED STATES POSTAL INSPECTOR

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 3rd day of May, 2022.

Karen E. Scott
UNITED STATES MAGISTRATE JUDGE